REMARKS

This is in response to the Office Action dated October 6, 2003. Claims 1 to 34 are pending. The Examiner's reconsideration of the rejections is respectfully requested in view of the remarks.

The drawings have been objected to; the Examiner stated that the memory storage device of claims 7, 13, 19, 25, and 31 and the steganographically embedding step of claims 16, 22, and 28 must be shown or the feature(s) cancelled from the claim(s). Respectfully, the steganographically embedding is depicted in at least Figures 1 and 5 at elements 110 and 912, respectively. The attached proposed drawing correction of Figure 1 shows a memory storage device. The Examiner's reconsideration of the objection is respectfully requested.

Claims 10, 16, 22, and 28 have been rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The Examiner stated that, with respect to claim 10, "the specification does not described steganographically hiding the encryption key in the first unit, it only discusses hiding the key in the second unit." Further, the Examiner stated, with respect to claims 16, 22, an 28, that "the specification does not describe embedding portions of the encryption key in the at least one first unit with respect to the base claims of the above claims. The specification does discuss embedding portions of the encryption key in the first and second units."

Claim 10 is supported in the specification at page 5, lines 4-5, among other places. Claims 16, 22, and 28 are supported in the specification at page 7, lines 20-21, among other places. The Examiner's reconsideration of the rejection is respectfully requested.

Claims 1 and 8 have been rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention. The Examiner stated essentially that claim 1 omits a connection between the scrambler and the steganographic unit and that claim 8 omits a connection between the key extractor and the descrambler. The Examiner further rejected claims 1 and 8 for being inconsistent.

Briefly, Applicant is unaware of any basis for rejecting an independent claim because of inconsistency with another independent claim. Respectfully, the scope of each independent claim should be determined on its own merit.

Referring to claim 1, the server includes a scrambler and a steganographic unit that each use an encryption key. Further still, the scrambler and the steganographic unit operate on units of a data stream. The scrambler and the steganographic unit are connected through the use of the encryption key and operations on units of the data stream.

Referring to claim 8, it is clear from the claim that a decoder connects the key extractor and the descrambler, wherein the claim recites, *inter alia*, "a decoder coupled to the key extractor and the descrambler..." Respectfully, the Examiner's reconsideration of the rejection is requested.

Claims 1, 2, 4-13, 16-20,, 22-26, 28-31, 33, and 34 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Ichikawa (U.S. Patent No. 5,872,846) in view of Orrin (U.S. Patent No. 6,011,849). The Examiner stated essentially that the combined teachings of Ichikawa and Orrin teach or suggest all the limitations of claims 1, 2, 4-13, 16-20, 22-26, 28-31, 33, and 34.

Claim 1 claims, *inter alia*, "a scrambler for encrypting at least one first unit using an encryption key; a steganographic unit for embedding the encryption key into at least one second unit for the data stream." Claims 20 and 33 recite, *inter alia*, "scrambling at least one first unit

by encrypting the at least one first unit using an encryption key; and steganographically embedding the encryption key into at least one second unit for the data stream."

Ichikawa teaches a dual key encryption method/system comprising a public key and a private key (see Figure 5). Ichikawa teaches a dual key encryption method, wherein two sets of asymmetric keys are implemented, one used for encrypting data and another used to encrypt a user specific key (see Figure 6 and col. 5 lines 44-64). Ichikawa does not teach or suggest "encrypting at least one first unit using an encryption key" and "embedding the encryption key into at least one second unit for the data stream" essentially as claimed in claims 1, 20, and 33. Ichikawa applies the same encryption method across the entire data stream. Therefore, Ichikawa fails to teach or suggest each limitation of claims 1, 20, and 33.

Orrin teaches a single key encryption method wherein an encryption key is used as a key and data to be encrypted (see col. 4, lines 45-64). Orrin teaches that an encryption algorithm creates the ciphertext, which is then steganograpgically secured (see col. 3, lines 1-64). Orrin applies a steganographic method to the same data that was encrypted (see Figures 4 and 5, and col. 4 line 45 to col. 5 lines 10). Orrin does not teach or suggest a first unit and a second unit of the data stream, much less "encrypting at least one first unit using an encryption key" and "embedding the encryption key into at least one second unit for the data stream" essentially as claimed in claims 1, 20, and 33. Orrin does not teach applying an encryption key to a first unit of the data stream and a steganographic method to a second unit of the data stream. Therefore, Orrin fails to cure the deficiencies of Ichikawa.

Referring now to claims 8, 26, and 34: claim 8 recites, *inter alia*, "a key extractor for extracting an encryption key steganographically hidden in at least one first unit in the data stream received from the server." Claims 26 and 34 claim, *inter alia*, "extracting an encryption key

steganographically embedded in at least one second unit in the data stream."

Ichikawa teaches a dual key encryption method, wherein two sets of asymmetric keys are implemented, one used for encrypting data and another used to encrypt a user specific key (see Figure 6 and col. 5 lines 44-64). Ichikawa does not teach or suggest a steganographic method/system. Ichikawa does not teach or suggest "extracting an encryption key steganographically" hidden or embedded in a unit of a data stream, essentially as claimed in claims 8, and 26 and 34, respectively. Therefore, Ichikawa fails to teach or suggest each limitation of claims 8, 26, and 34.

Orrin teaches that a key is encrypted and encoded steganographically into a data stream (see Figures 4 and 5 and col. 4 line 45 to col. 5 line 10). Orrin does not teach or suggest "a key extractor for extracting an encryption key steganographically hidden in at least one first unit in the data stream received from the server" as claimed in claim 8, or "extracting an encryption key steganographically embedded in at least one second unit in the data stream" as claimed in claims 26 and 34. Orrin does not teach that the encryption key is extracted from a first unit of the data stream steganographically, wherein the encryption key is used to decrypt a second unit of the data stream. Orrin does not teach a first unit and second unit of the data stream, essentially as claimed in claims 8, 26, and 34. Therefore, Orrin fails to cure the deficiencies of Ichikawa.

Claims 2, and 4-7 depend from claim 1. Claims 9-13 depend from claim 8. Claims 16-19 depend from claim 14. Claims 22-25 depend from claim 20. Claims 28-31 depend from claim 26. The dependent claims are believed to be allowable for at least the reasons given for claims 1, 8, 20, and 26 respectively. Claims 16-19 are believed to be allowable for at least the reasons given for claim 14 below. At least claims 5, 11, 17, 23, and 29 are believed to be allowable for additional reasons.

Claims 5, 11, 17, 23, and 29 claim, *inter alia*, "wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key."

Ichikawa teaches a dual key encryption method, wherein two sets of asymmetric keys are implemented, one used for encrypting data and another used to encrypt a user specific key (see Figure 6 and col. 5 lines 44-64). Ichikawa does not teach or suggest "wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key" as claimed in claims 5, 11, 17, 23, and 29. Ichikawa does not teach embedding or hiding an encryption key in an encrypted data stream. Therefore, Ichikawa fails to teach or suggest each limitation of claims 8, 26, and 34.

Orrin teaches that a key is encrypted and encoded steganographically into a data stream (see Figures 4 and 5 and col. 4 line 45 to col. 5 line 10). Orrin does not teach or suggest "wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key" as claimed in claims 5, 11, 17, 23, and 29. Orrin teaches that an encrypted encryption key is encoded steganographically into a data stream (see col. 6, lines 9-51 and col. 9, lines 34-42). Orrin does not teach that the encryption key is steganographically embedded or hidden in an encrypted data stream. Therefore, Orrin fails to cure the deficiencies of Ichikawa.

Claims 5, 11, 17, 23, and 29 are believed to be allowable over the combined teachings of Ichikawa and Orrin. Reconsideration of the rejection is respectfully requested.

Claims 3, 9, 14,15, 21, 27, and 32 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Ichikawa in view of Orrin and further in view of Katta et al. (U.S. Patent No. 5,621,799).

Claim 14 recites, *inter alia*, "segmenting the data into units for a data stream to be transferred over the link; scrambling at least one first unit by encrypting the at least one first unit using an encryption key; steganographically embedding the encryption key into at least one second unit for the data stream." Claim 32 claims, *inter alia*, "scrambling at least one first unit for the data stream before transmission by encrypting the at least one first unit using an encryption key; steganographically embedding the encryption key into at least one second unit for the data stream."

Ichikawa teaches a dual key encryption method, wherein two sets of asymmetric keys are implemented, one used for encrypting data and another used to encrypt a user specific key (see Figure 6 and col. 5 lines 44-64). Ichikawa does not teach or suggest a steganographic method/system. Ichikawa does not teach or suggest "steganographically embedding the encryption key into at least one second unit for the data stream" as claimed in claims 14 and 32. Therefore, Ichikawa fails to teach or suggest each limitation of claims 14 and 32.

Orrin teaches a single key encryption method wherein an encryption key is used as a key and data to be encrypted (see col. 4, lines 45-64). Orrin teaches that an encryption key is encrypted and encoded steganographically into a data stream (see Figures 4 and 5 and col. 4 line 45 to col. 5 line 10, and col. 8, lines 29-31). Orrin does not teach or suggest a first and a second unit of the data stream, much less "steganographically embedding the encryption key into at least one second unit for the data stream" as claimed in claims 14 and 32. Orrin does not teach applying an encryption key to a first unit of the data stream and a steganographic method to a second unit of the data stream. Therefore, Orrin fails to cure the deficiencies of Ichikawa.

Katta teaches system for transmitting a digital data containing variable length coding comprises a first scramble key generating means for generating a first scramble key at a first

predetermined interval; a second scramble key generation means for generating a second scramble key based on said first scramble key at a second predetermined interval smaller than said first predetermined interval; a scrambling means for scrambling said digital data based on said second scramble key (see col. 2, lines 30-45). Katta does not teach or suggest "encrypting the at least one first unit using an encryption key" and "steganographically embedding the encryption key into at least one second unit for the data stream", essentially as claimed in claims 14 and 32. Katta merely teaches the digital data to be scrambled has a variable length encoding. Applying a scrambling technique to digital data having a variable length encoding is not analogous to encrypting a first unit and steganographically encoding a second unit. Katta does not teach different scrambling being applied to different portions of the data. Therefore, Katta fails to cure the deficiencies of Ichikawa and Orrin.

Claim 3 depends from claim 1. Claim 9 depends from claim 8. Claim 15 depends from claim 14. Claim 21 depends from claim 20. Claim 27 depends from claim 26. The dependent claims are believed to be allowable for at least the reasons given for the independent claims. The Examiner's reconsideration of the rejection is respectfully requested.

Accordingly, claims 1 to 34 are believed to be allowable for at least the reasons stated. The Examiner's withdrawal of the rejections is respectfully requested. For the forgoing reasons, the application, including claims 1 to 34, is believed to be in condition for allowance. Early and favorable reconsideration is respectfully requested.

Respectfully submitted,

Nathaniel T. Wallace
Reg. No. 48,909
Attorney for Applicant

F. CHAU & ASSOCIATES, LLP
1900 Hempstead Turnpike, Suite 501
East Meadow, New York 11554
(516) 357-0091
(516) 357-0092 (FAX)

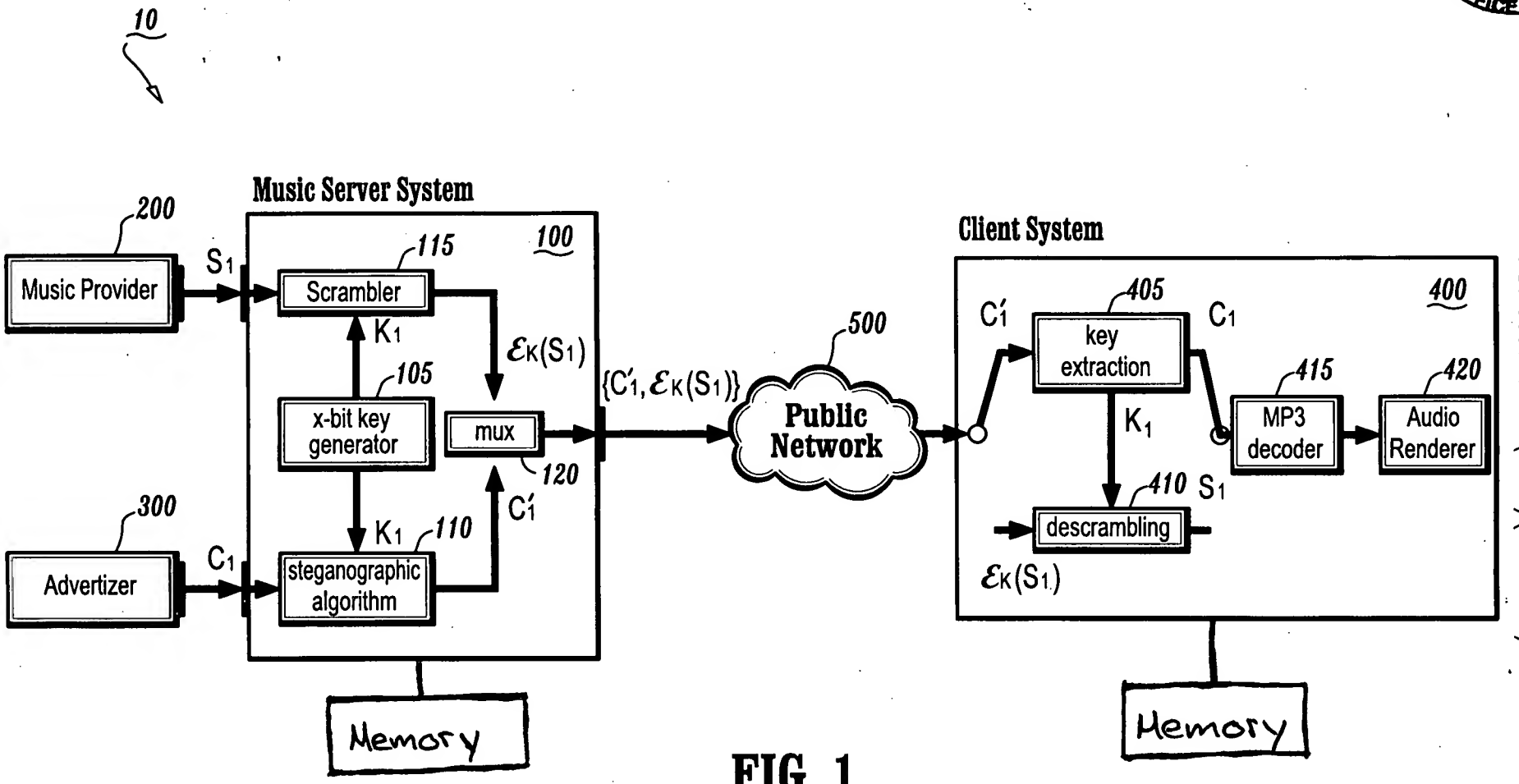

FIG. 1

(Proposed Correction)